UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,801	05/15/2006	Yong Ding	AFDC-00300	3452

34051 7590 10/30/2009

Stevens Law Group
1754 Technology Drive
Suite #226
San Jose, CA 95110

EXAMINER
LE, CANH

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
10/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/579,801	DING ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 8-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 8-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the communication filed on 02/18/2009.

Claims 1-4 and 8-16 have been examined and are pending.

Response to Arguments

Applicant's arguments, see pages 6-7, filed 07/24/2009, with respect to the 35 U.S.C. 112, 2nd rejection of claims 1-4 and 8-16 have been fully considered but they are not persuasive.

Claim recites the limitation "a signatory (S) selecting a braid ***x*** generated from the left subgroup $LB_m(l)$, a second braid ***x'*** generated from the braid group $B_n(l)$, and a third braid a generated from the braid group $B_n(l)$, by computer, wherein the computer is adapted to making them meet $x' = a^{-1}xa$, *moreover, with known x and x', it being* ***impossible*** *to* ***find a*** *in calculation*, and considering a braid pair (x', x) as a public key of signatory *(S), a* as a private key of signatory *(S)";* However, there is no further explanation in the specification how *with known x and x', it being* ***impossible*** *to* ***find a in calculation***, and considering a braid pair (x', x) as a public key of signatory *(S), a* as a private key of signatory *(S) (See paragraphs [0018], [0061] of publication specification)* (Emphasis added).

The applicant submits, in paragraph [0061] of publication specification, the present invention discloses: The called CSP problem means: for a given conjugacy pair (x,y) belongs to $B_n x B_n$ *(x~y),* finding a braid a belongs to B_n, which makes $y = a^{-1}xa$. For braid group, there is no efficient arithmetic which can solve the CSP problem in multinomial time currently, therefore,

for a conjugacy pair(x,y) belong to $B_n x B_n$ selected randomly, their CSP problem will be a difficult problem with high probability.

The Examiner takes a close look of the paragraph [0061] of publication specification. Although there is ***no efficient arithmetic*** which can solve the CSP problem in multinomial time currently therefore, for a conjugacy pair(x,y) belong to $B_n x B_n$ selected randomly, their CSP problem will be a ***difficult problem*** with high probability. The paragraph [0061] does not imply "*with known x and x', it being* ***impossible*** *to* ***find a*** *in calculation*, and considering a braid pair (x', x) as a public key of signatory *(S), a* as a private key of signatory *(S)".*

The Applicant has not provided the evidence to support "*with known x and x', it being* ***impossible*** *to* ***find a in calculation".*** Furthermore, the Applicant admits that it has not been solved by an efficient arithmetic that is widely-known by people of ordinary skill in the art. Therefore, it might be possible to "*find* ***a*** *in calculation"* in the aforementioned limitation.

It might be TRUE for the present time that "*with known x and x', it being* ***impossible*** *to* ***find a*** *in calculation ...".* However, it might be not be TRUE in the future, wherein a new technology or a new algorithm is invented to solve above problem.

Claims 2-4 and 13-14 are rejected due to virtual dependency of claim 1.

Claims 9-12 and 15-16 are rejected due to virtual dependency of claim 8.

Therefore, The 35 U.S.C. 112, 2nd rejection of claims 1-4 and 8-16 is maintained.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-4 and 8-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim recites the limitation "a signatory (S) selecting a braid ***x*** generated from the left subgroup $LB_m(l)$, a second braid ***x'*** generated from the braid group $B_n(l)$, and a third braid a generated from the braid group $B_n(l)$, by computer, wherein the computer is adapted to making them meet $x' = a^{-1}xa$, *moreover, with known x and x', it being* ***impossible*** *to* ***find a*** *in calculation*, and considering a braid pair (x', x) as a public key of signatory *(S), a* as a private key of signatory *(S)";* However, there is no further explanation in the specification how *with known x and x', it being* ***impossible*** *to* ***find a*** *in calculation*, and considering a braid pair (x', x) as a public key of signatory *(S), a* as a private key of signatory *(S) (See paragraph [0018], [0061] of publication specification)* (Emphasis added).

Claims 2-4 and 13-14 are rejected due to virtual dependency of claim 1.

Claims 9-12 and 15-16 are rejected due to virtual dependency of claim 8.

Allowable Subject Matter

Claims 1-4 and 8-16 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

Conclusion

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

October 27, 2009

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434